UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,185	07/30/2001	Edward B. Boden	END920010019US1	2635

7590 06/10/2005

IBM Corporation
Intellectual Property Law (Dept. 917, Bldg. 006-1)
3605 Highway 52 North
Rochester, MN 55901-7829

EXAMINER	
LESNIEWSKI, VICTOR D	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/919,185	BODEN, EDWARD B.	
	Examiner	Art Unit	
	Victor Lesniewski	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed 2/7/2005 has been placed of record in the file.

2. Claims 45-48 have been amended.

3. The rejection of claims 45-48 under 35 U.S.C. 101 is withdrawn in view of the amendment. The rejection of claim 44 under 35 U.S.C. 101 is maintained as discussed below.

4. Claims 1-53 are now pending.

5. The applicant's arguments, see pgs. 33-37, inter alia, of the amendment filed 2/7/2005, with respect to the rejection of claims 1-14, 16-27, 29-32, 34, and 36-53 under 35 U.S.C. 102(b) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. In turn, the rejection of claims 15, 28, 33, and 35 under 35 U.S.C. 103(a) is also withdrawn. Upon further consideration, a new grounds of rejection is made as will be discussed in detail below.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claim 44 remains rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 44 recites descriptive material that may or may not be an embodiment of a computer system or embodied on a computer readable medium so as to be executable. Here a program storage device readable by a machine does not suffice as computer readable or a computer program product and does not constitute eligible subject matter for patentability. See MPEP 2106.IV.B.1(a). It appears as though the applicant has amended claims 45-48 to add a computer readable medium, but has forgotten to amend claim 44.

8. Claims 49-53 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 49-53 recite descriptive material that may or may not be an embodiment of a computer system or embodied on a computer readable medium so as to be executable. It is unclear whether the computer program element is merely a software module or whether it is the same as a computer program product or a device that executes a computer readable medium. Thus a computer program element does not constitute eligible subject matter for patentability. See MPEP 2106.IV.B.1(a).

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-4, 6, 8, 10-14, 34, 36, 37, 43-45, 49, and 50 are rejected under 35 U.S.C. 102(e) as being anticipated by Lucovsky (U.S. Patent Number 6,868,450).

11. Lucovsky has disclosed:

- <Claim 1>

  A method for control and management of communication traffic, comprising the steps of: expressing access rules as filters referencing system kernel data (column 2, lines 13-35); for outbound processing, determining source application indicia (column 7, lines 51-65); for inbound packet processing, executing a look-ahead function to determine target

application indicia (column 8, lines 23-32); and responsive to said source or target application indicia, executing filter processing (column 8, lines 11-16 and 33-40).

- <Claim 2>

  The method of claim 1, further comprising the steps of executing said determining and executing steps within a kernel filtering function upon encountering a filter selector field referencing kernel data not included in said packet (column 8, lines 17-22).

- <Claim 3>

  The method of claim 1, said filter processing including the steps of: determining a task or thread identifier (figure 2, items 101 and 102); based on said task or thread identifier, determining a process or job identifier (column 4, lines 53-59); and based on said process or job identifier, determining job or process attributes for filter processing (column 7, lines 6-11 and figure 2, items 119 and 120).

- <Claim 4>

  The method of claim 1, said filter processing including the steps of: determining a user identifier (column 4, lines 53-59); and based on said user identifier, determining user attributes for filter processing (column 7, lines 6-11 and figure 2, items 119 and 120).

- <Claim 6>

  The method of claim 1, further comprising the steps for inbound processing of: passing an inbound packet to a sockets layer to identify said target application (column 5, lines 25-32 and column 8, lines 23-32).

- <Claim 8>

  The method of claim 1, further comprising the steps of: delivering to said filters infrastructure access rules for defining security context (column 1, lines 44-58 and column 2, lines 36-48).

- <Claim 10>

  A method for control and management of aspects of communication traffic within filtering, comprising the steps of: receiving IP packet data into a TCP/IP protocol stack executing within a system kernel (column 2, lines 13-35) executing filtering code within said system kernel with respect to non-IP packet data accessed within said system kernel outside of said TCP/IP protocol stack (column 8, lines 11-16 and 33-40).

- <Claim 11>

  The method of claim 10, said non-IP packet data including context data regarding said IP packet (column 8, lines 23-32).

- <Claim 12>

  The method claim 10, said non-IP packet data including data specific to a task generating said non-IP packet data (column 7, lines 51-65).

- <Claim 13>

  The method of claim 10, said non-IP packet data including data specific to a task that will receive said IP packet (column 8, lines 23-32).

- <Claim 14>

  The method of claim 11, said context data including packet arrival interface indicia (column 8, lines 23-32).

- <Claim 34>

  A method for control and management of communication traffic with respect to a system node, comprising the steps of: receiving at said system node an inbound packet (column 8, lines 23-32); and executing within a protocol stack of the system kernel of said system node a filtering function identifying for said inbound packet a filter referencing non-packet data (column 2, lines 13-35); and responsive to said filter, executing a look-ahead function for identifying a target application for said inbound packet (column 8, lines 23-32).

- <Claim 36>

  System for control and management of communication traffic, comprising: a system kernel including a filter function and stack data (column 2, lines 13-35); said filter function including a filter selectively referencing said stack data for expressing access rules (column 2, lines 13-35); said filter function being responsive to receipt of an outbound packet determining a source application (column 7, lines 51-65); said filter function being responsive to receipt of an inbound packet processing for executing a look-ahead function to determine a target application (column 8, lines 23-32); and said filter function being responsive to said source or target application for executing filter processing (column 8, lines 11-16 and 33-40).

- <Claim 37>

  A system for control and management of aspects of communication traffic within filtering, comprising: a system kernel (column 2, lines 13-35); a protocol stack executing within said system kernel for receiving IP packet data (column 2, lines 13-35); and

filtering code within said system kernel operable with respect to non-IP packet data accessed within said system kernel outside of said protocol stack for controlling and managing said aspects of communication traffic (column 2, lines 13-35).

- <Claim 43>

  A system for control and management of communication traffic with respect to a system node, comprising: a filtering function executing within a protocol stack of the system kernel of said system node identifying for an inbound packet a filter referencing non-packet data (column 2, lines 13-35 and column 8, lines 23-32); and a look-ahead function responsive to said filter for identifying a target application for said inbound packet (column 8, lines 23-32).

- <Claims 44 and 49>

  A computer program product or computer program element for control and management of communication traffic according to the steps comprising: expressing access rules as filters referencing system kernel data (column 2, lines 13-35); for outbound processing, determining a source application (column 7, lines 51-65); for inbound packet processing, executing a look-ahead function to determine a target application (column 8, lines 23-32); and responsive to said source or target application, executing filter processing (column 8, lines 11-16 and 33-40).

- <Claims 45 and 50>

  A computer program product or computer program element for control and management of aspects of communication traffic within filtering according to steps comprising: receiving IP packet data into a TCP/IP protocol stack executing within a system kernel

(column 2, lines 13-35) executing filtering code within said system kernel with respect to non-IP packet data accessed within said system kernel outside of said TCP/IP protocol stack (column 8, lines 11-16 and 33-40).

Since all the limitations of the invention as set forth in claims 1-4, 6, 8, 10-14, 34, 36, 37, 43-45, 49, and 50 were disclosed by Lucovsky, claims 1-4, 6, 8, 10-14, 34, 36, 37, 43-45, 49, and 50 are rejected.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 5, 7, 9, 22, 24-33, 35, 39, 41, 42, 47, 48, 52, and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lucovsky.

14. Concerning claims 5, 22, 24, 29, 39, 41, 42, 47, and 52, Lucovsky does not explicitly state determining a work control block. However, Lucovsky does state the use of multiple types of attributes and other identifiers in order to track a process in the system. The use of multiple processes, such as figure 2, items 101 and 102, with such attributes shows that Lucovsky's system in some way controls or coordinates the tasks or processes taking place. Thus it would be a clear extension of Lucovsky's system to be able to explicitly identify or determine this control during packet filtering. Thus, it would have been obvious to one of ordinary skill in the art at the

time of the applicant's invention to modify the system of Lucovsky by adding the ability to determine a work control block.

15. Concerning claims 7, 28, 33, and 35, Lucovsky does not explicitly state marking a packet as not deliverable before passing it to the sockets layer. However, taking some action on a packet before passing it on for further filtering is well known in the art and Lucovsky has disclosed a variety of features that could be used for such an action. In one instance Lucovsky discusses values that uniquely identify each process. See column 5, lines 18-24. For example, a packet could be marked as not deliverable before being passed to the sockets layer if its data does not correctly identify a certain value of a certain process. Also, authentication or authorization techniques are well known in the art that may lead to a pre-assessment of a packet before it is passed to the sockets layer. Thus, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the system of Lucovsky by adding the ability to mark a packet as not deliverable before passing it to the sockets layer.

16. Concerning claim 9, Lucovsky does not explicitly state logging, auditing, and filter rule load controls. However, Lucovsky does state the use of a database that controls the filtering and contains collected process attributes. It is well known in such system that monitor and control networks that such a central database may be logged, audited, or alternately loaded with certain controls by a system administrator or user, so it would be a clear extension of Lucovsky's system to add such features to his database. Thus, it would be obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the system of Lucovsky by adding logging, auditing, and filter rule load controls.

17. Thereby, Lucovsky discloses:

- <Claim 5>

  The method of claim 3, further comprising the step of determining from said task identifier a work control block containing said process or job identifier (column 4, lines 53-59 and obviousness).

- <Claim 7>

  The method of claim 6, further comprising the step of marking said inbound packet as not deliverable before passing it to said sockets layer (obviousness).

- <Claim 9>

  The method of claim 8, said infrastructure including logging, auditing, and filter rule load controls (figure 2, item 115 and obviousness).

- <Claim 22>

  A method for traversing a portion only of a protocol stack to disallow selective IP packet traffic, comprising the steps of: receiving a packet in the kernel of the operating system of a first node from an application, said kernel including filter processor (column 2, lines 13-35); for inbound packet processing to a first node from a second node, executing a look-ahead function in the system kernel of said first node to determining a target application (column 8, lines 23-32); for both said inbound packet processing, and for outbound packet processing from said first node to said second node, executing within said kernel the steps of processing said packet by determining a task ID (figure 2, items 101 and 102); responsive to said task ID, determining a corresponding work control block (column 4, lines 53-59 and obviousness); determining a user process or job identifier from said work control block (column 4, lines 53-59); from the user process or job

identifier selectively determining attributes for said user process or job (column 7, lines 6-11 and figure 2, items 119 and 120); and passing said attributes to said filter processor for managing and controlling communication traffic (column 8, lines 11-16 and 33-40).

- <Claim 24>

  A method for managing and controlling communication traffic by centralizing access rules in filters executing within and referencing data available in system kernels, comprising the steps for outbound packet processing from a first node to a second node of: receiving said packet in the kernel of the operating system of said first node from an application or process at said first node (column 7, lines 51-65); processing said packet by determining a task ID (figure 2, items 101 and 102); responsive to said task ID, determining a corresponding work control block (column 4, lines 53-59 and obviousness); responsive to said work control block, determining a process or job identifier (column 4, lines 53-59); responsive to said process job identifier, determining job or process attributes (column 7, lines 6-11 figure 2, items 119 and 120).

- <Claim 25>

  The method of claim 24, further comprising the steps for inbound packet processing from said second node to said first node of: initially operating said kernel at said first node to determine a target application for said packet at said first node (column 8, lines 23-32).

- <Claim 26>

  The method of claim 25, said initially operating step comprising executing a look-ahead function (column 8, lines 23-32).

- <Claim 27>

  The method of claim 26, said look-ahead function including the steps of operating a filter function to request of a sockets layer the identity of an application to which said sockets layer would pass said packet (column 5, lines 25-32 and column 8, lines 23-32).

- <Claim 28>

  The method of claim 27, further comprising the step of marking said packet as non-deliverable and thereafter passing said packet to said sockets layer to identify said application (obviousness).

- <Claim 29>

  A method for managing and controlling communication traffic by centralizing the access rules, comprising the steps for outbound packet processing from a first node to a second node of: receiving said packet in the kernel of the operating system of said first node from an application or process at said first node, said kernel including a filter processor (column 7, lines 51-65); processing said packet by determining a task ID (figure 2, items 101 and 102); responsive to said task ID, determining a corresponding work control block (column 4, lines 53-59 and obviousness); determining a user ID control block from said work control block (column 4, lines 53-59); from the user ID control block determining attributes for said user (column 7, lines 6-11 and figure 2, items 119 and 120); and passing said attributes to said filter processor for managing and controlling communication traffic (column 8, lines 11-16 and 33-40).

- <Claim 30>

  The method of claim 29, further comprising the steps for inbound packet processing from said second node to said first node of: initially operating said kernel at said first node to determine a target application for said packet at said first node (column 8, lines 23-32).

- <Claim 31>

  The method of claim 30, said initially operating step comprising executing a look-ahead function (column 8, lines 23-32).

- <Claim 32>

  The method of claim 31, said look-ahead function including the steps of operating a filter function to request of a sockets layer the identity of an application to which said sockets layer would pass said packet (column 5, lines 25-32 and column 8, lines 23-32).

- <Claim 33>

  The method of claim 32, further comprising the step of marking said packet as non-deliverable and thereafter passing said packet to said sockets layer to identify said application (obviousness).

- <Claim 35>

  The look-ahead function of the method of claim 34 further comprising the steps of: passing to a transport layer function identified by an IP header a packet marked non-deliverable for determining which user-level process or job is to receive said packet (obviousness); receiving from said transport layer an application layer task identifier said user-level process or job (column 8, lines 23-32 and figure 2, items 101 and 102); and

thereafter passing said packet marked by said task identifier to said transport layer for delivery to said application layer task (column 8, lines 33-40).

- <Claim 39>

  A system for traversing a portion only of a protocol stack to disallow selective IP packet traffic, comprising: a system kernel (column 2, lines 13-35); a filter processor executing within said system kernel (column 2, lines 13-35); said filter processor responsive to an inbound packet for executing a look-ahead function for determining a target application (column 8, lines 23-32); said filter processor responsive to both inbound and outbound packets for processing said packet by determining a task ID (figure 2, items 101 and 102); responsive to said task ID, determining a corresponding work control block (column 4, lines 53-59 and obviousness); determining a user ID, process or job identifier from said work control block (column 4, lines 53-59); from the user ID, process or job identifier selectively determining attributes for said user process or job (column 7, lines 6-11 and figure 2, items 119 and 120); and passing said attributes to said filter processor for managing and controlling communication traffic (column 8, lines 11-16 and 33-40).

- <Claim 41>

  A system for managing and controlling communication traffic by centralizing access rules in filters executing within and referencing data available in system kernels, comprising: code for receiving a packet in the kernel of the operating system of a first node from an application or process at said first node (column 8, lines 23-32); code for processing said packet by determining a task ID (figure 2, items 101 and 102); code responsive to said task ID for determining a corresponding work control block (column 4,

lines 53-59 and obviousness); code responsive to said work control block for determining a process or job identifier (column 4, lines 53-59); and code responsive to said process or job identifier for determining job or process attributes (column 7, lines 6-11 and figure 2, items 119 and 120).

- <Claim 42>

  A system for managing and controlling communication traffic by centralizing access rules, comprising: a first system node (figure 1, item 100); a second system node (figure 1, item 200); a kernel of the operating system of said first system node including a kernel filter processor (column 2, lines 13-35); said kernel for receiving from an application or process at said first system node a packet for communication to said second system node (column 7, lines 51-65); said kernel further for processing said packet by determining a task ID (figure 2, items 101 and 102); responsive to said task ID, determining a corresponding work control block (column 4, lines 53-59 and obviousness); determining a user ID control block from said work control block (column 4, lines 53-59); from the user ID control block determining attributes for said user (column 7, lines 6-11 and figure 2, items 119 and 120); and passing said attributes to said system kernel filter processor for managing and controlling communication traffic (column 8, lines 11-16 and 33-40).

- <Claims 47 and 52>

  A computer program product or computer program element for managing and controlling communication traffic by centralizing access rules in filters executing within and referencing data available in system kernels according to method steps comprising: receiving said packet in the kernel of the operating system of said first node from an

application or process at said first node (column 7, lines 51-65); processing said packet by determining a task ID (figure 2, items 101 and 102); responsive to said task ID, determining a corresponding work control block (column 4, lines 53-59 and obviousness); responsive to said work control block, determining a process or job identifier (column 4, lines 53-59); responsive to said process or job identifier, determining job or process attributes (column 7, lines 6-11 and figure 2, items 119 and 120).

- <Claims 48 and 53>

  The computer program product or element of claim 52, said method steps further comprising for inbound packet processing from said second node to said first node: initially operating said kernel at said first node to determine a target application for said packet at said first node (column 8, lines 23-32).

Since Lucovsky discloses all of the above limitations, claims 5, 7, 9, 22, 24-33, 35, 39, 41, 42, 47, 48, 52, and 53 are rejected.

18. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lucovsky, as applied above, in view of Wiegel (U.S. Patent Number 6,131,163).

19. Lucovsky disclosed a system for packet filtering based on a process attribute. In an analogous art, Wiegel disclosed packet filtering at a network gateway where received data is delivered to a network operating system.

20. Concerning claim 15, Lucovsky does not explicitly state the use of packet arrival time as a property for tracking data transmission in his system. However, Wiegel states the use of a

current time of day criteria in his security policy. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the system of Lucovsky by adding the ability to utilize a time-of-day property as provided by Wiegel. Here the combination satisfies the need for performing security checks at a low level of the operating system. See Wiegel, column 1, lines 56-67.

21. Thereby, the combination of Lucovsky and Wiegel discloses:

- <Claim 15>

  The method of claim 11, said context data including packet arrival time-of-day indicia (Wiegel, column 9, lines 39-46).

Since the combination of Lucovsky and Wiegel discloses all of the above limitations, claim 15 is rejected.

22. Claims 16-21, 23, 38, 40, 46, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lucovsky, as applied above, in view of Fiveash et al. (U.S. Patent Number 6,076,168), hereinafter referred to as Fiveash.

23. Lucovsky disclosed a system for packet filtering based on a process attribute. In an analogous art, Fiveash disclosed a method for securing data traffic between host systems that uses a filter having rules associated with a defined tunnel.

24. Concerning claims 16, 17, and 21, Lucovsky does not explicitly state establishing a tunnel between two IP addresses. However, he does discuss processes that operate between two unique port numbers. Furthermore, Fiveash's system is based on the use of a tunnel bound at each end to keep data confidential. It would have been obvious to one of ordinary skill in the art

at the time of the applicant's invention to modify the system of Lucovsky by adding the ability to establish a tunnel between two IP addresses as provided by Fiveash. Here the combination satisfies the need for a filter mechanism that can determine whether a process having a certain attribute may access a network. See Lucovsky, column 2, lines 5-10.

25. Concerning claims 18, 23, 38, 40, 46, and 51, Lucovsky does not explicitly state providing filter statements syntax for accepting parameters in the form of a selector. However, packet filtering systems that allow users to provide the parameters by using a filter statements syntax are well known in the art as evidenced by Fiveash. Fiveash states an exemplary list of rules that are used for filtering packets where the parameters of the rules are set by the user of the host system. See figure 4. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the system of Lucovsky by adding the ability to provide filter statements syntax for accepting parameters in the form of a selector as provided by Fiveash. Again the combination satisfies the need for a filter mechanism that can determine whether a process having a certain attribute may access a network. See Lucovsky, column 2, lines 5-10.

26. Thereby, the combination of Lucovsky and Fiveash discloses:

- <Claim 16>

  The method of claim 10, further comprising the steps of: establishing a tunnel between two IP address limiting traffic to applications bound to ports at each end of said tunnel (Lucovsky, column 5, lines 6-23 and Fiveash, column 3, lines 64-67); said filtering code accessing filtering attributes further limiting traffic selectively to job indicia (Lucovsky, column 4, lines 53-59 and column 7, lines 6-11).

- <Claim 17>

  The method of claim 10, further comprising the steps of: establishing a tunnel between two IP address limiting traffic to applications bound to ports at each end of said tunnel (Lucovsky, column 5, lines 6-23 and Fiveash, column 3, lines 64-67); and filtering code accessing filtering attributes further limiting traffic selectively to user identification indicia (Lucovsky, column 4, lines 53-59 and column 7, lines 6-11).

- <Claim 18>

  A method for centralizing system-wide communication management and control within filter rules, comprising the steps of: providing filter statements syntax for accepting parameters in the form of a selector, each selector specifying selector field, operator, and a set of values (Fiveash, figure 4); and said selector referencing data that does not exist in IP packets (Lucovsky, column 2, lines 13-35).

- <Claim 19>

  The method of claim 18, said parameters selectively including userid, user profile, user class, user group, user group authority, user special authority, job name, process name, job group, job class, job priority, other job or process attributes, and date & time (Lucovsky, column 4, lines 53-59).

- <Claim 20>

  The method of claim 18, said filters statements being provided within a user interface to said system (Fiveash, column 3, lines 57-58).

- <Claim 21>

  The method of claim 18, further comprising the steps of: establishing a tunnel between two IP address limiting traffic to applications bound to ports at each end of said tunnel (Lucovsky, column 5, lines 6-23 and Fiveash, column 3, lines 64-67); said filtering code accessing filtering attributes further limiting traffic selectively to job indicia (Lucovsky, column 4, lines 53-59 and column 7, lines 6-11); and operating said filtering code within a kernel filtering function upon encountering a filter selector field referencing kernel data not included in said traffic (Lucovsky, column 8, lines 11-16 and 33-40).

- <Claim 23>

  A method for expressing access rules as filters, comprising the steps of: providing a filter statements syntax for accepting parameters in the form of a selector, each selector specifying selector field, operator, and a set of values (Fiveash, figure 4); and said selector referencing data that does not exist in IP packets for controlling access to an application (Lucovsky, column 2, lines 13-35).

- <Claim 38>

  A system for centralizing system-wide communication management and control within filter rules, comprising: filter statements having a syntax for accepting parameters in the form of a selector, each selector specifying selector field, operator, and a set of values (Fiveash, figure 4); and said selector referencing data that does not exist in IP packets (Lucovsky, column 2, lines 13-35).

- <Claim 40>

  A system for expressing access rules as filters, comprising: a filter statements accepting parameters in the form of a selector, each selector specifying selector field, operator, and a set of values (Fiveash, figure 4); and said selector referencing data that does not exist in IP packets controlling access to an application (Lucovsky, column 2, lines 13-35).

- <Claims 46 and 51>

  A computer program product or computer program element for centralizing system-wide communication management and control within filter rules according to method steps comprising: providing filter statements syntax for accepting parameters in the form of a selector, each selector specifying selector field, operator, and a set of values (Fiveash, figure 4); and said selector referencing data that does not exist in IP packets (Lucovsky, column 2, lines 13-35).

Since the combination of Lucovsky and Fiveash discloses all of the above limitations, claims 16-21, 23, 38, 40, 46, and 51 are rejected.

Conclusion

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Victor Lesniewski whose telephone number is 571-272-3987. The examiner can normally be reached on Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

VL

Victor Lesniewski
Patent Examiner
Group Art Unit 2155

Bharat Barot.

BHARAT BAROT
PRIMARY EXAMINER